



# Department of Homeland Security Daily Open Source Infrastructure Report for 30 March 2006

Current  
Nationwide  
Threat Level is



[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The Lansing State Journal reports a stolen tanker truck that authorities were concerned could potentially be used as a weapon of mass destruction was found empty on Tuesday, March 28 at a gas station in northeastern Livingston County, Michigan. (See item [1](#))
- The Associated Press reports federal officials are investigating a possible safety breach involving two commercial planes at O'Hare International Airport, the third investigation of an apparent close call on the airfield's runways in less than a week. (See item [12](#))
- The St. Louis Post Dispatch reports the U.S. Centers for Disease Control and Prevention is planning to place antibiotics in 5,000 homes in the St. Louis area in a first-of-its kind test to learn how people would handle drugs given them to prepare for a bioterrorism attack. (See item [28](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *March 29, Lansing State Journal (MI)* — **Stolen fuel truck found in Michigan.** A stolen tanker truck authorities were concerned could "potentially be used as a weapon of mass destruction" was found Tuesday, March 28 at a Mobil gas station in northeastern Livingston

County, MI. The 2001 Freightliner was loaded with 2,000 gallons of fuel when it was taken Monday evening, March 27, in Oakland County. It was empty when it was found, said Trooper Jason Hoogstra. Oakland County Sheriff Michael Bouchard said the possibility that the thief was planning a terrorist act has not been ruled out. "It's a weapon on six wheels — if somebody had the know-how and inclination to do it," Hoogstra said of the tanker truck. Authorities said an Angelo Iafrate Construction Co. employee stated the truck was stolen sometime after 10:30 p.m. EST Monday from 2240 Avon Industrial Drive in Rochester Hills. A citizen spotted the tanker at the Mobil station. Bouchard's office has investigated other vehicle thefts, but none like this — where a vehicle was taken in such a short time and dumped of fuel. Bouchard said, "We never hope for thievery, but here, obviously given the current world we live in, that fuel (can be) taken for something other than fueling a vehicle."

Source: <http://www.lsj.com/apps/pbcs.dll/article?AID=/20060329/NEWS01/603290360/1001/news>

2. *March 29, Tribune–Democrat (PA)* — **Coal mine drill trains responders for emergency.**

About 48 emergency responders from ten mining companies received a telephone call early Tuesday, March 28, directing them to respond to a mine rescue at Seldom Seen Tourist Coal Mine in Pennsylvania. The men were told to rescue two boys, who entered the old underground mine in an attempt to steal copper wire. But an unexpected explosion filled the mine with smoke and dangerous gases — and both boys remained injured inside. And so the rescue drill began. The state's Bureau of Mine Safety, in conjunction with Mine Safety & Health Administration and the National Institute of Occupational Safety & Health, conducted the exercise to prepare coal miners for underground emergencies. The drill was designed to test response times and rescue abilities of state responders and mine-rescue teams.

Source: [http://www.tribune-democrat.com/homepage/local\\_story\\_088000317.html?keyword=leadpicturestory](http://www.tribune-democrat.com/homepage/local_story_088000317.html?keyword=leadpicturestory)

3. *March 28, Government Accountability Office* — **GAO–06–558T: Combating Nuclear Smuggling: Challenges Facing U.S. Efforts to Deploy Radiation Detection Equipment in Other Countries and in the United States (Testimony).** The Government Accountability Office (GAO) released two reports on U.S. efforts to combat nuclear smuggling in foreign countries and in the United States. Together with the March 2005 report on the Department of Energy's Megaports Initiative, these reports represent GAO's analysis of the U.S. effort to deploy radiation detection equipment worldwide. GAO's testimony discusses the progress made and challenges faced by the Departments of Energy (DOE), Defense, and State in providing radiation detection equipment to foreign countries, and the Department of Homeland Security's (DHS) efforts to install radiation detection equipment at U.S. ports of entry and challenges it faces. In the report on U.S. efforts to combat nuclear smuggling in other countries, GAO made five recommendations to improve, among other things, equipment maintenance, coordination among U.S. programs, and accountability of equipment. Both DOE and State agreed with GAO's recommendations. In the report on radiation detection at U.S. ports of entry, GAO made nine recommendations designed to help DHS speed up the pace of portal monitor deployments, better account for schedule delays and cost uncertainties, and improve its ability to interdict illicit nuclear materials. DHS agreed with GAO's recommendations.

Highlights: <http://www.gao.gov/highlights/d06558thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-558T>

4. *March 28, NBC 30 (CT)* — **Program encourages businesses to generate electricity.**

Businesses are being encouraged to generate their own electricity to save money and ease Connecticut's overburdened power system in a program approved Monday, March 27 by state regulators. So-called customer-side distributed generation is owned and operated by electric customers that could invest in equipment to generate electricity independently to provide some or all of their electricity needs. The state Department of Public Utility Control approved the program to meet requirements of legislation approved last year encouraging the development of new resources. Businesses could apply to state regulators for a grant of \$450 per kilowatt hour for heat and power generating plants and \$200 per kilowatt hour for emergency generators that typically operate during peak demand in summer months. Projects in southwest Connecticut, where electricity transmission bottlenecks are among the worst in New England, would receive an additional \$50 per kilowatt hour. Large generators of electricity could ultimately include hospitals, convention centers, condominiums and universities.

Source: [http://www.nbc30.com/news/8310604/detail.html?rss=har&psp=ne\\_ws](http://www.nbc30.com/news/8310604/detail.html?rss=har&psp=ne_ws)

5. *March 28, Reuters* — **New nuclear reactor plans raise questions.** The U.S. nuclear power industry is planning to build new reactors to produce cleaner electricity and reduce dependence on more expensive natural gas, raising questions about the safety of new plants. The Union of Concerned Scientists (UCS) aims to ensure that new reactors will not possess design flaws that must be corrected after they go into service, David Lochbaum, director of nuclear safety at UCS, said Tuesday, March 28. The Nuclear Energy Institute (NEI) anticipates utilities will build 12 to 15 new nuclear plants by 2015 to join the current 103 power reactors. Lochbaum questions whether ventilation systems at new plants built adjacent to existing reactors could protect control room operators from a radiation leak in an accident. "New reactors are designed to be safer than existing plants but when you build next to a reactor there is a potential for a bigger radioactive cloud. You have to build a stronger ventilation system," Lochbaum said. Radiation exposure could sideline plant operators and harm control room equipment. Cooling water systems for the new reactors, security to repel attacks, earthquake safety standards, and more nuclear waste to dispose of are other issues that need to be examined.

Source: [http://today.reuters.co.uk/news/newsArticle.aspx?type=scienc&NewsID=2006-03-28T221201Z\\_01\\_N28325308\\_RTRIDST\\_0\\_SCIE\\_NCE-UTILITIES-NUCLEAR-PLANTS-DC.XML&archived=False](http://today.reuters.co.uk/news/newsArticle.aspx?type=scienc&NewsID=2006-03-28T221201Z_01_N28325308_RTRIDST_0_SCIE_NCE-UTILITIES-NUCLEAR-PLANTS-DC.XML&archived=False)

6. *March 27, St. Petersburg Times (FL)* — **Trans-gulf pipeline scrutinized.** A proposal by the world's largest pipeline company to bring gasoline into Florida through a pipe under the Gulf of Mexico is facing growing resistance. Florida Governor Jeb Bush, who supported the plan when it was first made public just days after Hurricane Katrina, now opposes the idea. Saying a pipeline would consolidate rather than diversify the state's sources of gasoline, last week the governor said, "There has to be a different solution than the one that was suggested to me six months ago." Spot shortages and price spikes after Katrina had prompted Bush to call for more reliable state fuel supplies. Colonial Pipeline Co. of Alpharetta, GA, met with state officials last fall about a proposal for laying an underwater pipe from oil refineries on the Louisiana coast to the Tampa Bay area. One option called for Colonial's project to follow the path of the submerged 581-mile Gulfstream Natural Gas Pipeline that emerges at Port Manatee and became operational in May 2002. Susan Castiglione, spokesperson for Colonial, a consortium owned by six oil companies, said the company is still evaluating the cross-gulf proposal and has no timeline for making a decision.

Source: [http://www.thestate.com/mld/miamiherald/business/14181420.htm?source=rss&channel=miamiherald\\_business](http://www.thestate.com/mld/miamiherald/business/14181420.htm?source=rss&channel=miamiherald_business)

7. *March 14, Government Accountability Office* — **GAO-06-311: Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries (Report)**. According to the International Atomic Energy Agency, between 1993 and 2004, there were 662 confirmed cases of illicit trafficking in nuclear and radiological materials. Three U.S. agencies, the Departments of Energy (DOE), Defense, and State (State), have programs that provide radiation detection equipment and training to border security personnel in other countries. The Government Accountability Office (GAO) examined the progress U.S. programs have made in providing radiation detection equipment to foreign governments, including the current and expected costs of these programs; challenges U.S. programs face in this effort; and steps being taken to coordinate U.S. efforts to combat nuclear smuggling in other countries. GAO recommends to the Secretaries of Energy and State to integrate cost projections for anticorruption measures into long-term program cost estimates; upgrade less sophisticated portal monitors; provide maintenance for all handheld radiation detection equipment provided by U.S. programs; revise the interagency strategic plan; and compile, maintain, and share a master list of all U.S. radiation detection equipment assistance.

Highlights: <http://www.gao.gov/highlights/d06311high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-311>

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

8. *March 29, National Defense Magazine* — **Air Force modernization plans on track**. Analysts had warned in recent years that the Air Force should brace for drastic cuts in its aircraft procurement programs. The administration's proposed budget for fiscal year 2007, however, not only preserves the service's key acquisition accounts, but also contains seed money to begin research and development for new generations of aircraft. But the ramping up of new programs, such as a tanker replacement, a long-range bomber, and ongoing efforts such as the joint strike fighter and the F-22A Raptor, may mean some budget crunches in the near-term, experts predicted. Meanwhile, none of the Air Force's major programs face cancellation. The crunch will come in 2008, when many of the modernization programs begin in earnest, the analysts said. In the long term, renewed emphasis on unmanned aircraft and long-range strike could soon be competing for resources with manned fighter jets, said Michael O'Hanlon, senior fellow at the Brookings Institute. As unmanned reconnaissance capabilities increase, the need for remote sensing satellites may decrease, O'Hanlon said.

Source: [http://www.nationaldefensemagazine.org/issues/2006/april/air\\_force.htm](http://www.nationaldefensemagazine.org/issues/2006/april/air_force.htm)

## **Banking and Finance Sector**

9. *March 29, CNET News* — **Suffering in silence with data leaks.** The disclosure laws passed by 23 states during the past three years have had little impact when it comes to ensuring consumers are notified about data theft or loss. The majority of state laws allow a company to stay mum about a robbery, if disclosing it would interfere with a police investigation. That's a huge loophole that could be used in almost every incidence of stolen data, said Dan Clements, of CardCops.com. "Only about ten percent of the merchants do the right thing and notify customers when there is a compromise," Clements said. To understand the problem with disclosure laws around the U.S., California's SB 1386 is a good place to start, because most other state laws were patterned after it. The law allows a merchant to stay quiet about a digital data breach if the information lost was encrypted. The state law is also unclear on the issue of a merchant's responsibility, if the company's technology provider suffered an intrusion.  
Source: [http://news.com.com/2102-1029\\_3-6055160.html?tag=st.util.pri nt](http://news.com.com/2102-1029_3-6055160.html?tag=st.util.pri nt)

10. *March 29, ZDNet Australia* — **Australian Tax Office bars Trojan-infected tax agents.** The Australian Tax Office has restricted access to its website after discovering that a "small number" of tax agents have been infected by a Trojan, which has "stolen" their user IDs and passwords. Troj/Dumaru-BZ has infected a small number of tax agents' computer systems compromising their Tax Agent Portal user ID and password details. According to anti-virus firm Sophos, the Trojan is capable of capturing data in various forms, including information copied on a clipboard and "protected storage area of Windows," as well as cached passwords. Dumaru "looks" for financial information stored in certain applications, such as E-Gold, WebMoney, Total Commander, and Far Manager.  
Source: [http://www.zdnet.com.au/news/security/soa/ATO\\_bars\\_Trojan\\_in\\_fected\\_tax\\_agents/0.2000061744.39248671.00.htm](http://www.zdnet.com.au/news/security/soa/ATO_bars_Trojan_in_fected_tax_agents/0.2000061744.39248671.00.htm)

11. *March 29, New York Times* — **U.S. arrests seven on charges of credit data trading.** The Secret Service on Tuesday, March 28 announced seven arrests as part of a continuing crackdown on online forums where credit card data and other stolen consumer information is routinely traded. A total of 21 people have been arrested in the U.S. and Britain in the last three months in the undercover operation, the agency said. It is the largest federal law enforcement action taken against the thriving online trade in credit card numbers, bank accounts, passwords, personal identification numbers, and other data since an earlier effort, Operation Firewall, broke up the largest black market trading board, Shadowcrew.com, in 2004. Jonathan Cherry, a spokesperson for the Secret Service, said the new crackdown, called Operation Rolling Stone, was aimed at "online criminal enterprises that threaten our financial infrastructure." The arrests yesterday were made in Florida, New York, Illinois, Pennsylvania, California, and Washington on a variety of state and federal charges related to online identity theft, credit card, and access device fraud, Cherry said. Some of the people arrested have been linked to the compromise of hundreds of thousands of debit card numbers and personal identification numbers. The precise source of the security breaches has not been determined.  
Source: [http://news.com.com/U.S.+arrests+7+on+charges+of+credit+data+trading/2100-7348\\_3-6055261.html?tag=nefd.top](http://news.com.com/U.S.+arrests+7+on+charges+of+credit+data+trading/2100-7348_3-6055261.html?tag=nefd.top)

## **Transportation and Border Security Sector**

**12. *March 29, Associated Press* — FAA investigates third close call on O'Hare runways.**

Federal officials are investigating a possible safety breach involving two commercial planes at O'Hare International Airport, the third investigation of an apparent close call on the airfield's runways in less than a week. Federal Aviation Administration (FAA) officials said Tuesday, March 28, that they are trying to determine whether two planes that were preparing for takeoff on Sunday, March 26, got closer than allowed under federal rules. An Airbus A320 plane had been cleared for takeoff at around 12:20 p.m. CST but was told to abort its takeoff four seconds later because another plane had been readying for takeoff on an intersecting runway, the FAA said. FAA spokesperson Tony Molinaro said Tuesday that the planes got no closer than 1,100 feet apart. He said officials do not yet know if that violated federal separation rules, which dictate how close planes can come to one another while on the ground. The latest investigation comes as federal investigators look into two separate runway incidents at O'Hare last week. The FAA and National Transportation Safety Board consider runway incursions the top threat to airport safety.

Source: [http://www.usatoday.com/travel/flights/2006-03-29-ohare-safety\\_x.htm](http://www.usatoday.com/travel/flights/2006-03-29-ohare-safety_x.htm)

**13. *March 29, Department of Transportation* — Florida receives \$480 million for repairing hurricane-damaged traffic signals and highways.** Florida is receiving \$480 million to pay the state's cost for replacing traffic signals, clearing highway debris and repairing roads in 21 counties devastated by Hurricanes Rita and Wilma, Department of Transportation Secretary Norman Y. Mineta said on Wednesday, March 29. High winds from last year's hurricanes swept northeast across Florida, causing widespread damage to more than two thousand traffic signals in Broward and Palm Beach Counties alone. The federal transportation funds will reimburse the state for repairing or replacing the damaged traffic signals and highway signs, restoring washed out highways, and clearing downed trees, sand and other debris from roads immediately after the storms. This funding is part of an emergency highway aid package for Gulf Coast states requested by President Bush and approved by Congress the end of last year, according to Mineta.

Source: <http://www.dot.gov/affairs/dot4406.htm>

**14. *March 29, Department of Transportation* — Alabama receives \$17.6 million for Hurricane Katrina road damages.** Alabama is receiving \$17.6 million to pay the state's cost for repairing the Cochrane Bridge, interstate ramps, traffic signals and other highway damage caused by Hurricane Katrina, Department of Transportation Secretary Norman Y. Mineta said on Wednesday, March 29. An offshore oil platform dislodged by Katrina's high winds slammed into the Cochrane Bridge over Mobile Bay, damaging its cable system and concrete structure. The federal funds will reimburse the state for repairing the Bridge and for new ramps connecting U.S. 90 and Interstate 10, replacing or repairing damaged traffic signals and highway message signs, and the cost of clearing downed trees, sand and other debris from roads immediately after the storm.

Source: <http://www.dot.gov/affairs/dot4506.htm>

15. *March 29, Reuters* — **U.S. airlines vie for China routes.** After a 14-year wait to get into the world's most populous country, AMR Corp.'s American Airlines — which set up a Beijing office more than a decade ago in a bid to build relationships — on Sunday, April 2, is scheduled to start flying up to 245 passengers a day to the fast-growing U.S. trading partner. Profitable international routes are crucial to U.S. carriers' efforts to climb back to profitability after years of surging fuel costs and increased competition from low-cost carriers on domestic routes knocked them deeply into the red. The U.S. and China are set to hold aviation market liberalization talks next month, and U.S. airlines will be there to press their case for allowing more flights, sooner.

Source: [http://biz.yahoo.com/rb/060329/airlines\\_china.html?.v=1](http://biz.yahoo.com/rb/060329/airlines_china.html?.v=1)

16. *March 29, Government Accountability Office* — **GAO-06-471: Undeclared Hazardous Materials: New DOT Efforts May Provide Additional Information on Undeclared Shipments (Report).** Each year, an estimated three billion tons of regulated Hazmat are transported in the U.S. Under federal law, these materials must be properly declared, packaged, and labeled. In addition, federal officials know that undeclared shipments of Hazmat also occur, either out of shippers' lack of knowledge or economic motivations. Shipments of undeclared hazardous materials—materials not properly packaged, labeled, and otherwise identified as hazardous—pose a serious safety and security concern for transportation workers, emergency responders, and the general public should an accident or incident occur. Department of Transportation (DOT) officials report that since the terrorist attacks of September 11, 2001, the security of such shipments, especially those that can be used as weapons of mass destruction, has attracted the attention of the transportation community, government officials, and emergency responders. DOT has new efforts under way that officials expect will enhance the current approach for discovering undeclared Hazmat entering the United States: The Government Accountability Office requested comments on a draft of this report from DOT and the Department of Homeland Security (DHS). DOT offered a number of technical comments that were incorporated, as appropriate. DHS did not provide comments on this report.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-471>

17. *March 29, Government Accountability Office* — **GAO-06-557T: Passenger Rail Security: Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts (Testimony).** The July 2005 bombing attacks on London's subway system dramatically revealed the vulnerability of passenger rail systems worldwide to terrorist attacks and demonstrated the need for an increased focus on security for these systems. This testimony, which is based primarily on the Government Accountability Office's (GAO) September 2005 report on passenger rail security (GAO-05-851), provides information on (1) the security practices that domestic and selected foreign rail transit operators have implemented to mitigate risks and enhance security; (2) the Department of Homeland Security's (DHS) and the Department of Transportation's (DOT) funding of rail transit security and use of risk management in funding decisions; and (3) the steps DHS and DOT have taken to improve coordination on rail transit security matters. As part of its 2005 report, GAO contacted 32 U.S. rail transit operators and 13 passenger rail operators in seven European and Asian countries. GAO's September 2005 report on passenger rail security recommended, among other things, that the Secretary of Homeland Security, in collaboration with DOT, determine the feasibility of implementing certain rail security practices used in foreign countries. DHS and DOT generally agreed with the report's recommendations.

Highlights: <http://www.gao.gov/highlights/d06557thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-557T>

18. *March 29, Government Accountability Office* — **GAO-06-574T: Next Generation Air Transportation System: Preliminary Analysis of the Joint Planning and Development Office's Planning, Progress, and Challenges (Testimony)**. The health of the nation's air transportation system is critical to its citizens and economy. However, the current approach to managing air transportation is becoming increasingly inefficient and operationally obsolete. In 2003, Congress created the Joint Planning and Development Office (JPDO) to coordinate the federal and nonfederal stakeholders necessary to plan and implement a transition from the current air transportation system to the "next generation air transportation system" (NGATS). JPDO, although housed within the Federal Aviation Administration (FAA), has seven partner agencies: the Departments of Transportation, Commerce, Defense, and Homeland Security; FAA; the National Aeronautics and Space Administration (NASA); and the White House Office of Science and Technology Policy. This testimony provides preliminary results from the Government Accountability Office's (GAO) ongoing study of the status of JPDO's efforts. GAO provides information on (1) the extent to which JPDO is facilitating the federal interagency collaboration and aligning the human and financial resources needed to plan and implement the NGATS, (2) the actions taken by JPDO to adequately involve stakeholders in the planning process, and (3) the extent to which JPDO is conducting the technical planning needed to develop the NGATS.

Highlights: <http://www.gao.gov/highlights/d06574thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-574T>

19. *March 28, Associated Press* — **Police plan Metro sweep for morning rush**. Washington, DC's Metro transit police increased their visibility Wednesday, March 29, with a special detail sweeping a station during the morning rush. The detail included a dog team and as many as 20 officers who spread out along the station platform to inspect all trains. The officers normally work at Metro headquarters. The patrols will continue indefinitely on random days.

Source: [http://www.wusatv9.com/news/news\\_article.aspx?storyid=48025](http://www.wusatv9.com/news/news_article.aspx?storyid=48025)

20. *March 28, New York Daily News* — **Anti-terror plan for underwater subways**. Girding for a terrorist attack, the Metropolitan Transportation Authority (MTA) plans to bolster underwater subway tunnels with layers of concrete and dirt to stop any flooding from a bomb blast. Two MTA committees on Monday, March 27, approved a \$17.1 million contract for a Staten Island marine firm to build the anti-terror bulwarks. The MTA has 14 underwater subway tunnels, many dug through solid rock. They run under the East River, the Harlem River, and the Newtown Creek on the Queens-Brooklyn border. The MTA committees also approved \$80 million worth of work to add 399 surveillance cameras and 425 motion sensors to the system to thwart terror attacks.

Source: <http://www.nydailynews.com/03-28-2006/news/local/story/403560p-341813c.html>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

Nothing to report.

## **Agriculture Sector**

21. *March 26, Canadian Press* — **Virulent pig bacteria in Canada.** A virulent new strain of a common pig virus is wreaking havoc on Ontario, Canada, hog herds. Tens of thousands of hogs have been removed from farms by deadstock companies this winter and last year. They are victims of a new strain of porcine circovirus or other illnesses that the autoimmune disease brings on or makes worse. Larry Skinner, chair of Ontario Pork's board, said province-wide mortality rates are running at 10 to 12 percent — five to six times above the norm on affected farms. On the hardest-hit farms, the figure is 40 to 50 percent or more. Porcine circovirus, or PCVII, is not new; in fact, it's a common bug found in pigs. But something happened to it 18 months ago: PCVII had previously been confined to hogs aged six to 10 weeks, but it began showing up in hogs aged 10 to 15 weeks and was resistant to traditional vaccines. PCVII information: <http://duke.usask.ca/~misra/virology/stud2005/swine/porcinecircovirus.html>  
Source: [http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article\\_Type1&c=Article&cid=1143327032650&call\\_pa\\_geid=970599119419](http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1143327032650&call_pa_geid=970599119419)
22. *March 24, Associated Press* — **Four farms quarantined because of tuberculosis-infected hogs.** Four West Virginia farms have been quarantined following the discovery of tuberculosis (TB) in hogs illegally imported from Ohio, Department of Agriculture Commissioner Gus R. Douglass announced Friday, March 24. The quarantine includes two farms in Putnam County and one each in Logan and Greenbrier counties, agency spokesperson Buddy Davidson said. Animals can't be moved on or off the premises until further notice. The hogs were brought into the state on March 13 by Red House resident Tim Reedy, who is cooperating with the Department of Agriculture. Reed bought the hogs in Hillsborough, OH, Davidson said. He did not know what type of facility sold the hogs but said it was probably a farm. Davidson said the hogs did not have health certificates verifying that they had been tested for diseases and immunized. The agency has notified agriculture officials in Ohio, as well as in three other states because Reedy sold one hog in Pennsylvania, six in Kentucky and 14 in Virginia. State food safety personnel discovered signs of tuberculosis on Tuesday, March 21, in hogs being processed at custom meat plants.  
Source: <http://www.kentucky.com/mld/kentucky/news/14179781.htm>

## **Food Sector**

23. *March 29, Agence France-Presse* — **Japan, U.S. take small steps to resume U.S. beef sales.** Japan and the U.S. have agreed on new measures to ease fears in Japan of mad cow disease in U.S. beef but failed to set a timetable to resume U.S. beef imports. Farm, foreign and health ministry officials of the two governments concluded a two-day meeting in Tokyo on Wednesday, March 29. Japan, once the biggest foreign market for U.S. beef, has repeatedly refused to resume imports, which it abruptly banned in January after a shipment violated safety guidelines that require the removal of risky body parts. The two sides agreed on additional

measures to prevent a similar violation, including a training program for exporters and a new verification system that would increase checks on U.S. beef exports. The United States will begin taking the measures shortly, while the Japanese government will hold public hearings to monitor people's views of the preventive measures.

Source: [http://news.yahoo.com/s/afp/20060329/hl\\_afp/healthjapanustrade\\_060329111726;\\_ylt=Aoy3Q\\_MqHTXQ5GwNFuHtkkSJOrgF:\\_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/afp/20060329/hl_afp/healthjapanustrade_060329111726;_ylt=Aoy3Q_MqHTXQ5GwNFuHtkkSJOrgF:_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--)

[\[Return to top\]](#)

## **Water Sector**

24. *March 29, Associated Press* — **Teens arrested in water facility break-in.** Authorities charged two teenagers in connection with a break-in at a water facility and expected to charge a third as more than 9,000 Blackstone, MA, area residents waited Wednesday, March 29, to hear if their drinking water had been contaminated. The teens are suspected of cutting the barbed wire at the facility Monday, March 27, cutting lines to an alarm, and then damaging an electrical panel and a vent at the top of a 1.3-million-gallon water storage tank, said Blackstone Police Lt. Gregory Gilmore. A five-gallon container with an odor was found on top of the tank, but authorities do not yet know what, if anything, was put into the water. Gilmore said the teens became suspects after talking about the incident at school. The two 15-year-old boys, whose names were not released because of their ages, were charged with malicious destruction of property, tampering with a public water supply and polluting the water supply, all felonies, and trespassing, Gilmore said. He said a 15-year-old girl had not been arrested but likely would be charged with trespassing.

Source: <http://www.breitbart.com/news/2006/03/29/D8GL9V3G5.html>

[\[Return to top\]](#)

## **Public Health Sector**

25. *March 29, Reuters* — **Bird flu found in poultry in Baghdad.** Iraq has found the H5N1 bird flu virus in poultry in Baghdad, said the government spokesperson of the Higher Committee on Bird Flu on Wednesday, March 29. Ibtissam Aziz said in a statement that tests had proved that the H5N1 strain of the virus existed in one of the birds in an area in Baghdad.

Source: <http://www.alertnet.org/thenews/newsdesk/L29744927.htm>

26. *March 29, Associated Press* — **New Orleans health care still in shambles.** The city of New Orleans has only 456 staffed hospital beds, compared with 2,269 before the city was struck by Hurricane Katrina. While emergency care is available, auditors noted that patients at two hospitals waited up to two hours to be unloaded from ambulances. They also found patients being kept and treated in the emergency room because beds weren't available elsewhere. When auditors visited New Orleans, they found primary and emergency health care was available, but access to specialty care was quite limited. The city also relied on a network of clinics to treat poor patients before the hurricane, but more than three quarters of those clinics are closed. About 19 clinics are open now, but they generally operate at less than half of capacity.

Report: <http://www.gao.gov/new.items/d06576r.pdf>

Source: <http://www.cbsnews.com/stories/2006/03/29/ap/national/mainD8 GKV4886.shtml>

27. *March 28, Radio Sweden* — **Bird flu detected in Swedish mink.** Swedish authorities say they have found a wild mink infected with bird flu, suspected to be the deadly H5N1 strain. It's the first time in Sweden that a highly pathogenic version of the H5 virus has been confirmed in an animal other than a bird. Dozens of birds in Sweden have tested positive for the H5N1 virus.  
Source: <http://www.sr.se/cgi-bin/International/nyhetssidor/artikel.asp?ProgramID=2054&Nyheter=&artikel=825481>
28. *March 28, St. Louis Post Dispatch* — **St. Louis will be part of bioterrorism study.** The U.S. Centers for Disease Control and Prevention (CDC) is planning to place antibiotics in 5,000 homes in the St. Louis, MO, area in a first-of-its kind test to learn how people would handle drugs given them to prepare for a bioterrorism attack. Starting next month, some 20,000 people will be screened to see which households receive "MedKits" that contain antibiotics for each member of the family. Households will be randomly selected from three groups: public health responders such as firefighters; workers at a single, as yet unidentified corporation; and recipients of publicly funded health care at clinics. The pilot project is aimed at finding the best way to distribute drugs in case of emergencies and whether people would store the drugs properly and save them for when they are needed. The MedKits will contain either Doxycycline or Ciprofloxacin, better known as Cipro. Doxycycline is often mentioned as a treatment for anthrax, among other bacteria. Cipro also could be used to ward off infections from a variety of intentionally introduced agents, including plague, smallpox, botulism and tularemia. Family members will go through medical screening before being chosen.  
Source: <http://www.stltoday.com/stltoday/news/stories.nsf/nation/story/D7E2276B883CAED686257140001F232D?OpenDocument>
29. *March 28, Channel News Asia* — **Hand, foot and mouth disease cases continue to climb.** The number of hand, foot and mouth disease cases has continued to increase in Singapore, with 785 cases reported last week. According to the Health Ministry, this is more than double the number of cases in the preceding week. It is also significantly higher than the weekly average of 113 in January and 174 in February this year. Almost 3,000 cases of hand, foot and mouth disease have been reported since January this year.  
Source: <http://www.channelnewsasia.com/stories/singaporelocalnews/view/200340/1/.html>

[\[Return to top\]](#)

## **Government Sector**

Nothing to report.

[\[Return to top\]](#)

## **Emergency Services Sector**

30. *March 29, National Defense Magazine* — **DHS vows to reform disaster response.** With hurricane season fast approaching, Department of Homeland Security (DHS) officials are

promising to apply lessons learned from last year's Katrina disaster by putting key reforms in place before June 1. At the top of DHS Secretary Michael Chertoff's list is replacing the Federal Emergency Management Agency's (FEMA) outdated computer and commodity tracking system. DHS will also end the practice of entering into ad hoc trucking contracts through the Department of Transportation. In addition, FEMA will end its reliance on volunteer organizations such as the Red Cross to gather information.

Source: <http://www.nationaldefensemagazine.org/issues/2006/april/sb-beat.htm#dhs>

31. *March 29, San Francisco Chronicle* — **Scientists re-create action of 1906 earthquake.** Less than four seconds after the ground ruptured off San Francisco's coast on April 18, 1906, much of San Francisco was destroyed. The great quake that struck before dawn that day savaged the entire Bay Area within 30 seconds and ripped the Earth's surface for 300 miles along the San Andreas Fault at speeds up to 13,000 mph. For the first time, scientists have re-created in extraordinary detail what happened to the Earth's quiet surface that spring day nearly a century ago. A new computer simulation of the quake's ground-shaking violence overlayed on today's Bay Area — and from Cape Mendocino in the north to San Juan Bautista in the south — offers scientists, engineers and disaster workers the ability to predict where the ground will shake most severely. That knowledge will help engineers design safer buildings and guide first responders as they decide where best to focus their efforts. The unprecedented scientific effort, described Tuesday, March 28, by its creators, took two years and the combined power of supercomputers at four institutions, teams of geophysicists and mathematicians.

For further detail on this effort: <http://earthquake.usgs.gov/regional/nca/1906/simulations/>

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/03/29/QUAKE.TMP>

32. *March 28, Sentinel (PA)* — **Pennsylvania anti-terrorism group to stand up Infra Watch Program.** Last year, the South Central Pennsylvania Counter-Terrorism Task Force (SCTF) had "lots of successes" and "lots of challenges," SCTF officials indicated at a Homeland Security Conference at Harrisburg, PA, Area Community College Monday, March 27. The conference, which runs through Thursday, March 30, includes additional training. Courses range from "Hospital Evacuation Strategies" to "Care of Animals During a Disaster" and "Managing a Food Contamination Incident." The task force will continue to focus on private industry and critical infrastructure facilities, said Ted Wise, executive director of the Cumberland County Office of Emergency Preparedness. It has facilitated exercises and training sessions covering topics such as terrorism prevention and awareness, security vulnerability and agricultural terrorism. The task force is also planning to start an "Infra Watch Program," similar to neighborhood watches but, instead, organizing people to keep an eye on electric power grids, bridges, water supplies and the like, Wise said.

Source: <http://www.cumberlink.com/articles/2006/03/28/news/news26.txt>

33. *March 28, Weekly (GA)* — **FEMA releases preparedness DVD.** With The Department of Homeland Security's Federal Emergency Management Agency (FEMA) facing the upcoming 2006 hurricane season, a new citizen preparedness DVD entitled, "Getting Ready For Disaster — One Family's Experience" is ready for distribution to help citizens get ready for natural and man-made disasters. The DVD guides viewers through important steps of disaster preparedness and brings into focus issues such as drafting a family disaster plan, stockpiling food and water, helping children cope with disasters and preparedness for special populations such as the elderly and people with disabilities. The DVD is not limited to hurricane preparedness; rather, it

follows FEMA's all hazards approach to disaster preparedness. The content is based on the most reliable hazard awareness and emergency education information, such as the latest scientific knowledge and physical research on what happens in disasters.

Source: <http://www.theweekly.com/news/2006/March/28/FEMA.html>

- 34. *March 27, Reno Gazette-Journal* — Rural first responders in Nevada have the worst response times in the nation.** Nevada's rural — and largely volunteer — ambulance crews are facing an uphill battle to get state help reducing their longest-in-the-nation response times, leading lawmakers say. A Reno Gazette-Journal analysis of the federal Fatality Analysis Reporting System and U.S. Department of Transportation data found that Nevada's response to rural fatal accidents is more than 18 minutes — 56 percent longer than the U.S. average for rural fatalities and 44 percent longer than for other Western states. The analysis showed response time for all-volunteer crews — which tend to be in the most sparsely populated counties — is twice as long as it is for predominately paid crews. The three-month investigation also revealed many rural emergency medical service crews are driving old and unreliable vehicles, borrowing vital rescue equipment from neighboring counties, suffering repeated communication breakdowns and struggling to fill their volunteer rosters because of stricter post-9/11 training requirements enacted by the state.

Source: <http://news.rgj.com/apps/pbcs.dll/article?AID=/20060327/NEWS10/603270334/1016/NEWS>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

- 35. *March 28, FrSIRT* — F-Secure Messaging Security Gateway Sendmail code execution vulnerability.** A vulnerability in Sendmail may permit a specially crafted attack to take over the Sendmail MTA process, allowing a remote user to execute commands and run arbitrary programs on the system. Analysis: F-Secure Messaging Security Gateway Appliances use Sendmail. The vulnerability may permit a specially crafted attack to take over the Sendmail MTA process, allowing a remote user to execute commands and run arbitrary programs on the system. Affected products: F-Secure Messaging Security Gateway X200 version 3.1.0 and prior; F-Secure Messaging Security Gateway X200 version 3.2.4 and prior; F-Secure Messaging Security Gateway P600 version 3.1.0 and prior; F-Secure Messaging Security Gateway P600 version 3.2.4 and prior; F-Secure Messaging Security Gateway P800 version 3.1.0 and prior; F-Secure Messaging Security Gateway P800 version 3.2.4 and prior. Solution: Hotfixes are automatically distributed through the delivery system.

Source: <http://www.fsirt.com/english/advisories/2006/1139>

- 36. *March 28, Hackers Center* — Linux kernel IP ID value increment weakness.** A weakness in the Linux kernel, which can be exploited to disclose certain system information and potentially to bypass certain security restrictions. Analysis: The weakness is caused due to an error within the "ip\_push\_pending\_frames()" function when creating a packet in reply to a received SYN/ACK packet. This causes RST packets to be sent with a IP ID value that is incremented per packet. This can potentially be exploited to conduct idle scan attacks. Affected products: Linux Kernel 2.4.x; Linux Kernel 2.6.x. Solution: Update to version 2.6.16.1:

<http://www.kernel.org/>

Secunia is currently not aware of any official patches for the 2.4 kernel.

Source: <http://www.hackerscenter.com/archive/view.asp?id=23887>

37. *March 28, Hackers Center* — **Sun Solaris process environment disclosure security issue.** A security issue has been reported in Sun Solaris, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information. Analysis: The security issue is caused due to the "/usr/ucb/ps" command revealing the environment variables and values of all processes to an unprivileged user when run with the "-e" option. This can potentially reveal certain information of processes that belong to the root user. Affected: Sun Solaris 8 and Sun Solaris 9. Solution: Apply patches. See source advisory for further solution details.  
Source: <http://www.hackerscenter.com/archive/view.asp?id=23886>

38. *March 28, Tech Web* — **Security firm releases patch for zero-day Internet Explorer flaw.** EEye Digital Security has released a temporary patch for a zero-day vulnerability in Internet Explorer (IE) that is being used by malicious Websites to install spyware on users' computers, officials said Tuesday, March 28. The eEye patch is meant as a placeholder until Microsoft Corp. releases a permanent fix, which is expected by Tuesday, April 11, said Marc Maiffret, co-founder and chief hacking officer of eEye. At that time, users of the eEye patch are advised to use the add/remove program in Windows to delete the fix before installing the Microsoft patch. The vulnerability, called the CreateTextRange bug, enables hackers to exploit active scripting in IE to install keystroke loggers and other malicious software.  
Source: <http://www.securitypipeline.com/news/184400787;jsessionid=PDRAQICTESZRYQSNDBECKICCIJUMKJVN>

39. *March 28, Electric News* — **Australia tackles spam with new code.** Australia has cracked down on junk mail with what is believed to be the world's first industry code for tackling spam. Under the new code, Internet service providers (ISPs) will bear some of the responsibility for helping fight spam. Service providers must offer spam-filtering options to their subscribers and advise them on how to best deal with and report the nuisance mail. In addition to Australian ISPs, global e-mail operators like MSN Hotmail and Yahoo will be hit by the legislation.  
Source: <http://www.electricnews.net/frontpage/news-9676885.html>

40. *March 28, Computer World* — **Two DNS servers hit by denial-of-service attacks.** In the second attack of its kind in the past few days, Domain Name System servers at Network Solutions Inc. were hit by a denial-of-service attack Tuesday afternoon, March 28, resulting in a brief performance degradation for customers, according to the company. The attacks, which started at around 2:20 p.m. EST, were targeted at the company's WorldNIC name servers and resulted in a service degradation for about 25 minutes before the server was restored to normal, a spokesperson for the company said. Over the weekend, Joker.com, a domain-name registrar in Germany, was hit with a similar distributed denial-of-service attack that disrupted service to customers.  
Source: <http://www.computerworld.com/developmenttopics/websitegmt/story/0,10801,109972,00.html>

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles the createTextRange() DHTML method. By persuading a user to access a specially crafted webpage, a remote, unauthenticated attacker may be able to execute arbitrary code on that user's system. This vulnerability can also be used to crash Internet Explorer. We are aware of proof of concept code for this vulnerability. More information about the reported vulnerability can be found in the following US-CERT Vulnerability Note:

VU#876678 – Microsoft Internet Explorer createTextRange() vulnerability  
<http://www.kb.cert.org/vuls/id/876678>

Known attack vectors for this vulnerability require Active Scripting to be enabled in Internet Explorer. Disabling Active Scripting will reduce the chances of exploitation. Until an update, patch or more information becomes available, US-CERT recommends disabling Active Scripting as specified in the Securing Your Web Browser document.

[http://www.us-cert.gov/reading\\_room/securing\\_browser/#how\\_to\\_secure](http://www.us-cert.gov/reading_room/securing_browser/#how_to_secure)

We will continue to update current activity as more information becomes available.

### **TSP Phishing Scams**

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. Recently, the phishing scam targeted the Thrift Savings Plan (TSP), a retirement savings plan for United States government employees and members of the uniformed services. For more information please see Thrift Savings Plan (TSP) at URL: <http://www.tsp.gov/>

If you were affected by the TSP phishing scam, please refer to the TSP E-mail scam instructions for assistance. <http://www.tsp.gov/curinfo/emailscam.html>

US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.  
[http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html)

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Additionally, users are encouraged to take the following measures to prevent

phishing attacks from occurring:

Do not follow unsolicited web links received in email messages.

Contact your financial institution immediately if you believe your account and/or financial information has been compromised.

#### Current Port Attacks

<b>Top 10 Target Ports</b>	1026 (win-rpc), 6881 (bittorrent), 25 (smtp), 3800 (----), 445 (microsoft-ds), 41170 (----), 49200 (----), 80 (www), 14256 (----), 32778 (sometimes-rpc19)
----------------------------	--

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

41. *March 29, Sun Chronicle (MA)* — **Security scrutiny at the mall.** North Attleboro, MA's police officers are keeping a close eye on Emerald Square mall without even leaving the police station. Surveillance cameras have been installed outside the Route 1 mall beaming images of activity outside the mall in "real time" to police dispatchers 24 hours a day, seven days a week. "The purpose is to increase the awareness of security at the Emerald Square mall," Police Chief Michael P. Gould said. He noted the regional mall has been identified as a potential target of terrorism. Gould said the system will enable public safety officials to better respond in the event of a major crisis, such as a chemical spill. Gould said the system can be expanded to other areas in town, now that the network infrastructure is in place. Thus, more security cameras could be installed at other critical locations, such as the town's electric department substations and municipal water facilities, he said.

Source: [http://www.thesunchronicle.com/articles/2006/03/28/city/city\\_3.txt](http://www.thesunchronicle.com/articles/2006/03/28/city/city_3.txt)

[[Return to top](#)]

## **General Sector**

Nothing to report.

[[Return to top](#)]

## **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.